AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for facilitating access to a plurality of applications that require passwords, comprising:

receiving a request for a password from an application running on a remote computer system, the request being received at a local computer system, wherein the request for the password includes computer code that when run on the local computer system requests the password on behalf of the application on the remote computer system;

authenticating the request as originating from a trusted source, wherein authenticating the request involves authenticating the remote computer system that sent the request by verifying a digital signature and certificate chain for the remote computer system, thereby determining if the node is authorized to access the application;

using an identifier for the application to look up the password for the application in a password store containing a plurality of passwords associated with the plurality of applications, wherein the plurality of passwords allows a different password to be used with each application of the plurality of applications; and

if the password exists in the password store, sending the password or a function of the password to the application on the remote computer system.

2. (Cancelled)

3. (Currently amended) The method of ~~claim 2~~ claim 1, wherein the computer code is in the form of a platform-independent applet that runs on a platform-independent virtual machine on the local computer system.

4. (Previously presented) The method of claim 3, wherein sending the password or the function of the password to the application to the remote computer system involves:

communicating the password to the platform-independent applet; and

allowing the platform-independent applet to forward the password to the application on the remote computer system.

5. (Previously presented) The method of claim 3, wherein the platform-independent applet is a signed platform-independent applet, and wherein authenticating the request includes authenticating the platform-independent applet's certificate chain.

6. (Original) The method of claim 1, wherein authenticating the request involves authenticating a creator of the request.

7 (Canceled).

8. (Original) The method of claim 1, further comprising, if the password store is being accessed for the first time,

prompting a user for a single sign on password for the password store; and

using the single sign on password to open the password store.

9. (Original) The method of claim 8, wherein if a time out period for the password store expires,

prompting the user again for the single sign on password for the password store; and

using the single sign on password to open the password store.

10. (Previously presented) The method of claim 1, wherein if the password store is being accessed for the first time, the method further comprises authenticating the user through an authentication mechanism, wherein the authentication mechanism includes one of:

a smart card;

a biometric authentication mechanism; and

a public key infrastructure.

11. (Original) The method of claim 1, wherein if the password does not exist in the password store, the method further comprises:

adding the password to the password store; and

sending the password to the application on the remote computer system.

12. (Original) The method of claim 11, wherein adding the password to the password store further comprises automatically generating the password.

13. (Original) The method of claim 11, wherein adding the password to the password store further comprises asking a user to provide the password.

14. (Original) The method of claim 1, further comprising decrypting data in the password store prior to looking up the password in the password store.

15. (Original) The method of claim 1, wherein the password store is located on a second remote computer system.

16. (Previously presented) The method of claim 1, wherein the password store is located on one of:

a local smart card;

a removable storage medium; and

a memory button.

17. (Original) The method of claim 1, further comprising:

receiving a request to change the password from the application on the remote computer system;

automatically generating a replacement password;

storing the replacement password in the password store; and

forwarding the replacement password or the password function to the application on the remote computer system.

18. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating access to a plurality of applications that require passwords, the method comprising:

receiving a request for a password from an application running on a remote computer system, the request being received at a local computer system, wherein the request for the password includes computer code that when run on the local computer system requests the password on behalf of the application on the remote computer system;

authenticating the request as originating from a trusted source , wherein authenticating the request involves authenticating the remote computer system that sent the request by verifying a digital signature and certificate chain for the remote computer system, thereby determining if the node is authorized to access the application;

using an identifier for the application to look up the password for the application in a password store containing a plurality of passwords associated with the plurality of applications, wherein the plurality of passwords allows a different password to be used with each application of the plurality of applications; and

if the password exists in the password store, sending the password or a function of the password to the application on the remote computer system.

19. (Cancelled)

20. (Currently amended) The computer-readable storage medium of ~~claim 19~~ claim 18, wherein the computer code is in the form of a platform-independent applet that runs on a platform-independent virtual machine on the local computer system.

21. (Previously presented) The computer-readable storage medium of claim 20, wherein sending the password or the function of the password to the application to the remote computer system involves:

communicating the password to the platform-independent applet; and

allowing the platform-independent applet to forward the password to the application on the remote computer system.

22. (Previously presented) The computer-readable storage medium of claim 20, wherein the platform-independent applet is a signed platform-independent applet, and wherein authenticating the request includes authenticating the platform-independent applet's certificate chain.

23. (Original) The computer-readable storage medium of claim 18, wherein authenticating the request involves authenticating a creator of the request.

24 (Canceled).

25. (Original) The computer-readable storage medium of claim 18, wherein the method further comprises, if the password store is being accessed for the first time,

prompting a user for a single sign on password for the password store; and

using the single sign on password to open the password store.

26. (Original) The computer-readable storage medium of claim 25, wherein if a time out period for the password store expires, the method further comprises:

prompting the user again for the single sign on password for the password store; and

using the single sign on password to open the password store.

27. (Previously presented) The computer-readable storage medium of claim 18, wherein if the password store is being accessed for the first time, the method further comprises authenticating the user through an authentication mechanism, wherein the authentication mechanism includes one of:

a smart card;

a biometric authentication mechanism; and

a public key infrastructure.

28. (Original) The computer-readable storage medium of claim 18, wherein if the password does not exist in the password store, the method further comprises:

adding the password to the password store; and

sending the password to the application on the remote computer system.

29. (Original) The computer-readable storage medium of claim 28, wherein adding the password to the password store further comprises automatically generating the password.

30. (Original) The computer-readable storage medium of claim 28, wherein adding the password to the password store further comprises asking a user to provide the password.

31. (Original) The computer-readable storage medium of claim 18, wherein the method further comprises decrypting data in the password store prior to looking up the password in the password store.

32. (Original) The computer-readable storage medium of claim 18, wherein the password store is located on a second remote computer system.

33. (Previously presented) The computer readable storage medium of claim 18, wherein the password store is located on one of:

a local smart card;

a removable storage medium; and

a memory button.

34. (Original) The computer-readable storage medium of claim 18, wherein the method further comprises:

receiving a request to change the password from the application on the remote computer system;

automatically generating a replacement password;

storing the replacement password in the password store; and forwarding the replacement password or the password function to the application on the remote computer system.

35. (Currently amended) An apparatus that facilitates accessing a plurality of applications that require passwords, comprising:

a receiving mechanism that receives a request for a password from an application running on a remote computer system, the request being received at a local computer system, wherein the request for the password includes computer code that when run on the local computer system requests the password on behalf of the application on the remote computer system;

an authentication mechanism that authenticates the request as originating from a trusted source, wherein the authentication mechanism is configured to authenticate the remote computer system that sent the request by verifying a digital signature and certificate chain for the remote computer system, thereby determining if the node is authorized to access the application;

a lookup mechanism that uses an identifier for the application to look up the password for the application in a password store containing a plurality of passwords associated with the plurality of applications, wherein the plurality of passwords allows a different password to be used with each application of the plurality of applications; and

a forwarding mechanism that sends the password to the application on the remote computer system if the password exists in the password store.

36. (Cancelled)

37. (Currently amended) The apparatus of ~~claim 36~~ claim 35, wherein the computer code is in the form of a platform-independent applet that runs on a platform-independent virtual machine on the local computer system.

38. (Previously presented) The apparatus of claim 37, wherein the forwarding mechanism is configured to send the password to the application on the remote computer system by:

communicating the password to the platform-independent applet; and

allowing the platform-independent applet to forward the password to the application on the remote computer system.

39. (Previously presented) The apparatus of claim 37, wherein the platform-independent applet is a signed platform-independent applet, and wherein the authentication mechanism is configured to authenticate a certificate chain.

40. (Original) The apparatus of claim 35, wherein the authentication mechanism is configured to authenticate a creator of the request.

41 (Canceled).

42. (Original) The apparatus of claim 35, wherein if the password store is being accessed for the first time, the lookup mechanism is configured to:

prompt a user for a single sign on password for the password store; and to

use the single sign on password to open the password store.

43. (Original) The apparatus of claim 42, wherein if a time out period for the password store expires, the lookup mechanism is configured to:

prompt the user again for the single sign on password for the password store; and to

use the single sign on password to open the password store.

44. (Previously presented) The apparatus of claim 35, wherein if the password store is being accessed for the first time, the lookup mechanism is configured to authenticate the user through an authentication mechanism, wherein the authentication mechanism includes one of:

a smart card;

a biometric authentication mechanism; and

a public key infrastructure.

45. (Original) The apparatus of claim 35, further comprising an insertion mechanism, wherein if the password does not exist in the password store the insertion mechanism is configured to:

add the password to the password store; and to

send the password to the application on the remote computer system.

46. (Original) The apparatus of claim 45, wherein the insertion mechanism is additionally configured to automatically generate the password.

47. (Original) The apparatus of claim 45, wherein the insertion mechanism is additionally configured to ask a user to provide the password.

48. (Original) The apparatus of claim 35, further comprising a decryption mechanism that is configured to decrypt data in the password store.

49. (Original) The apparatus of claim 35, wherein the password store is located on a second remote computer system.

50. (Previously presented) The apparatus of claim 35, wherein the password store is located on one of:

a local smart card;

a removable storage medium; and

a memory button.

51. (Original) The apparatus of claim 35, further comprising a password changing mechanism that is configured to:

receive a request to change the password from the application on the remote computer system;

automatically generate a replacement password;

store the replacement password in the password store; and to

forward the replacement password to the application on the remote computer system.

52. (Currently amended) A method for facilitating access to a plurality of applications that require passwords, comprising:

receiving a request to look up a password at a password server, wherein the request is received from computer code running on the client that requests the password on behalf of the application;

authenticating the request as originating from a trusted source, wherein authenticating the request involves authenticating the remote computer system that sent the request by verifying a digital signature and certificate chain for the remote computer system, thereby determining if the node is authorized to access the application;

wherein the request is received from a client and includes an identifier for an application requesting the password from the client;

using the identifier for the application to look up the password for the application in a password store containing a plurality of passwords associated with the plurality of applications, wherein the plurality of passwords allows a different password to be used with each application of the plurality of applications; and

if the password exists in the password store, sending the password or a function of the password to the client, so that the client can present the password to the application.

53. (Cancelled)

54. (Currently amended) The method of ~~claim 53~~ claim 52, wherein the computer code is in the form of a platform-independent applet that runs on a platform-independent virtual machine on the client.

55. (Currently amended) A server that distributes code for facilitating access to a plurality of applications that require passwords, wherein the code operates by:

receiving a request for a password from an application running on a remote computer system, the request being received at a local computer system, wherein the request includes computer code that when run on the local computer system requests the password on behalf of the application on the remote computer system;

authenticating the request as originating from a trusted source, wherein authenticating the request involves authenticating the remote computer system that sent the request by verifying a digital signature and certificate chain for the remote computer system, thereby determining if the node is authorized to access the application;

using an identifier for the application to look up the password for the application in a password store containing a plurality of passwords associated with the plurality of applications, wherein the plurality of passwords allows a different password to be used with each application of the plurality of applications; and

if the password exists in the password store, sending the password or a function of the password to the application on the remote computer system.